Translating Security Requirements into Protection Profiles

Peter C. Sargent
PreVal Specialist, Inc.
preval@att.net
443-742-4430

AGENDA

- **How to create a PP**

- **Purpose**

- **Reason for caring**

- **Examples**

- **Benefits**

- **Future**

How We Do This ?

- **<u>A FOUR STEP PROCESS</u>**

  - **STEP A**

    - **Identify Requirements in language understood by creators of product or users of product**

    - **Allows the community to identify requirements without having to know Common Criteria.**

How We Do This ? (2)

– **STEP B**

- **Translate your product/system requirements to CC language**

- **Identify existing elemental PPs that might answer need**

- **Map the results of those that do not have existing PP to new PPs**

How We Do This ? (3)

- STEP C

  - **Evaluate the PP for Common Criteria Compliance**

  - **Create PP's that meet NIAP requirements while including requirements of target audience**

  - **Not everything in original list will make the PP**

How We Do This ? (4)

- STEP D

  - Vett the PP to a large, knowledgeable audience for comments

  - Create PP's that reflect needs and requirements of broad spectrum of users

  - Try to make generic enough to go beyond original audience. May or may not work!!

PURPOSE

- **Enhance understanding of products and systems relative to security functionality**

- **Train all sides to recognize and understand CC terminology**

- **Give vendors CC requirements to meet**

- **Provide "Corporate" and acquisition personnel with a more powerful mechanism for understanding and comparison**

WHY SHOULD WE CARE ?

- **NSTISSP 11 requirements for CC and CMVP Validation!   www.nstissc.gov**

- **NSA/DoD desire for protection profiles!**

- **Federal (Especially Homeland Security) desire for protection profiles!**

- **Commercial (Healthcare, Insurance, Banking) desire for protection profiles!**

EXAMPLES OF PPs

- **Can get on the Information Assurance Technical Framework Forum (IATF) website (www.iatf.net), click on Protection Profiles in documents**

EXAMPLES OF PP Development

- **Let's look at "one" example -**

  Intrusion Detection

- **There are now Three PPs**

- **Started as one in 1998**

Examples of PP Development (Cont'd)

- **STEP A**

- Input from Army, Navy, Marine Corps, and Joint Chiefs.

- Each had identified products and listed the functionality of each. Also identified other requirements

Examples of PP Development (Cont'd)

- **Step B:**
  - PP written from Product Lists from Services, and Requirements ID'd in other Documents provided
  - Written to include Protection, not just detection as this was identified

Examples of PP Development (Cont'd)

Step C:

- **Evaluated for CC compliance**
- **Comment returned on inclusions, not just CC compliance**
- **Addressed comments**

Examples of PP Development (Cont'd)

Step D:

- **No vetting with the Services, or any other knowledgeable audience**

Examples of PP Development (Cont'd)

- **Federal Agency System Architecture PP**
    - **Started with Agency Security Requirements**
    - **Mapped requirements to existing Elemental PPs**
    - **Identified some aspects of elemental PPs that do not need to be utilized in all cases – I&A, Audit,etc.**
    - **Identified requirements with no existing Elemental PPs**
    - **Wrote elemental PPs to fulfill these security requirements**
    - **Submitted System PP to agency personnel for review, with mapping to requirements submitted**
    - **Still in process – No plans to send through NIAP review**

Examples of other input to PP Process

- **FIPS 140-2 validation for Cryptography**
- **Privacy requirements – current ANSI X9 Working Group**
- **Wireless Working Group proposed for ANSI X9F**
- **Homeland Security Initiatives**
- **IATF Forum has had programs on Wireless and PKI**
- **Healthcare HIPAA requirements**
- **Insurance Industry starting to identify needs**

BENEFITS OF PP Development

- **Enhance "Corporate" understanding of CC and inter-relationship of products**

- **Security needs in a Common Standardized Language will create more uniform types of products that will lead to interoperability – but this is Not Guaranteed**

FUTURE OF PP's

- **Better Exchange of Security Requirements**

    – **By "Corporate Interests"**
    – **By Vendors**
    – **By Acquisition Personnel**
    – **By Users**

CONTACT US

PreVal Specialist, Inc.
214 Kennedy Dr.
Severna Park, MD
21146
443-742-4430
preval@att.net